

Ngày 10 tháng 3 năm 2022

GÓP Ý CỦA LIÊN MINH PHẦN MỀM (BSA) VỀ DỰ THẢO LUẬT BẢO VỆ QUYỀN LỢI NGƯỜI TIÊU DÙNG

Kính gửi: Bộ Công Thương

BSA | Liên minh Phần mềm (**BSA**)[1] trân trọng cảm ơn Bộ Công Thương (**Bộ CT**) vì đã cho chúng tôi cơ hội đóng góp ý kiến với dự thảo Luật Bảo vệ quyền lợi người tiêu dùng (**LBVQLNTD 2022**). BSA là tổ chức hàng đầu hỗ trợ ngành công nghiệp phần mềm toàn cầu trước chính phủ và trên thị trường quốc tế. Các thành viên của BSA là những công ty sáng tạo nhất thế giới, tạo ra các giải pháp phần mềm mà giúp các doanh nghiệp thuộc mọi quy mô trong mọi thành phần của nền kinh tế hiện đại hóa và phát triển.

BSA ủng hộ việc Chính phủ Việt Nam thu thập ý kiến đóng góp của các bên liên quan đối với LBVQLNTD 2022. Chúng tôi hiểu rằng LBVQLNTD 2022 nhằm thay thế Luật bảo vệ quyền lợi người tiêu dùng hiện hành được ban hành vào năm 2010. LBVQLNTD 2022 đề xuất các nghĩa vụ mới đối với "nền tảng trung gian trực tuyến" và "nền tảng trung gian trực tuyến lớn", cũng như các điều khoản liên quan tới việc bảo vệ thông tin cá nhân của người tiêu dùng.

BSA nhận thấy rằng việc ban hành các chính sách và quy định hợp lý để bảo vệ người tiêu dùng là thiết yếu trong thời đại thương mại điện tử, nhằm bảo vệ người tiêu dùng một cách hiệu quả trong môi trường kỹ thuật số. Nếu được điều chỉnh thích hợp, các chính sách như vậy có thể giúp phát triển một nền kinh tế kỹ thuật số trong nước sôi động và đổi mới, đồng thời tạo ra sự tin tưởng lớn hơn vào việc sử dụng các công nghệ để tạo điều kiện cho việc áp dụng các dịch vụ hỗ trợ phần mềm an toàn và hiệu quả. Do đó, điều quan trọng là phải đảm bảo rằng LBVQLNTD 2022 không đặt ra các yêu cầu vô lý hoặc quá khắt khe đối với các sản phẩm và dịch vụ hỗ trợ phần mềm, và đặc biệt là những yêu cầu được thiết kế để hỗ trợ khách hàng doanh nghiệp. Các nghĩa vụ bảo vệ dữ liệu trong LBVQLNTD 2022 cũng phải phù hợp với dự thảo Nghị định bảo vệ dữ liệu cá nhân (**Nghị định BVDLCN**)[2] của Việt Nam và tương thích với pháp luật bảo vệ dữ liệu quốc tế. Nếu không, những nghĩa vụ này sẽ cản trở khả năng của chính các doanh nghiệp Việt Nam trong việc tham gia hiệu quả vào nền kinh tế kỹ thuật số đang phát triển mạnh mẽ của Việt Nam.

Tóm tắt các Khuyến nghị của BSA

BSA khuyến nghị những điều sau:

---

[1] Thành viên của BSA bao gồm: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, và Zoom Video Communications, Inc.

[2] BSA lưu ý rằng Chính phủ Việt Nam vừa ban hành Nghị quyết số 27/NQ-CP thông qua Hồ sơ xây dựng dự thảo Nghị định BVDLCN, và Bộ trưởng Bộ Công an hiện được giao nhiệm vụ báo cáo và xin ý kiến Ủy ban Thường vụ Quốc hội về việc ban hành Nghị định BVDLCN.

300 Beach Road
#30-06 The Concourse
Singapore 199555
P: +65 6292 2072
F: +65 6292 6369
W: bsa.org
Regional Representative Office
UEN: S97RF0005K

- Điều chỉnh các định nghĩa có phạm vi quá rộng và không rõ ràng trong LBVQLNTD 2022 để loại trừ một cách rõ ràng các công ty cung cấp các dịch vụ được thiết kế cho khách hàng doanh nghiệp,[3] trái ngược với người tiêu dùng cá nhân, từ phạm vi pháp luật;
- Phân biệt giữa các chủ thể quyết định cách thức và lý do thu thập thông tin cá nhân (**bên kiểm soát dữ liệu**) và chủ thể chỉ đơn giản xử lý những thông tin cá nhân đã được thu thập thay mặt cho một công ty khác (**bên xử lý dữ liệu**) và loại trừ bên xử lý dữ liệu khỏi các nghĩa vụ cụ thể trong LBVQLNTD 2022;[4] và
- Loại bỏ Điều 9 của LBVQLNTD 2022 về yêu cầu sự đồng ý để tránh nhầm lẫn và mâu thuẫn với dự thảo Nghị Định BVDLCN.

Điều chỉnh định nghĩa và loại trừ các nhà cung cấp dịch vụ doanh nghiệp

LBVQLNTD 2022 đặt ra các định nghĩa cho "tổ chức kinh doanh",[5] "nền tảng trung gian trực tuyến",[6] and "nền tảng trung gian trực tuyến lớn".[7] Những định nghĩa này mang tính rộng mở và áp đặt các nghĩa vụ lên các chủ thể không tương tác với người tiêu dùng cá nhân, chẳng hạn như nhà cung cấp dịch vụ doanh nghiệp. Do đó, BSA khuyến nghị rằng các định nghĩa trong LBVQLNTD 2022 nên được điều chỉnh để loại trừ các nhà cung cấp dịch vụ doanh nghiệp khỏi phạm vi điều chỉnh.

Các dịch vụ doanh nghiệp hoặc dịch vụ doanh nghiệp với doanh nghiệp (**B2B**) tạo điều kiện hoạt động của nhiều tổ chức trên khắp thế giới, bao gồm các doanh nghiệp vừa và nhỏ và các công ty lớn, chính quyền địa phương và trung ương, bệnh viện, trường học, trường đại học và các tổ chức phi lợi nhuận. Khác với dịch vụ tập trung vào người tiêu dùng – dịch vụ cung cấp trực tiếp cho người dùng cuối cá nhân, dịch vụ doanh nghiệp chỉ dành cho đối tượng khách hàng là các tổ chức thuộc mọi quy mô và trên tất cả các ngành nhằm giúp họ hoạt động an toàn và hiệu quả, cải thiện năng suất, tăng cường phát triển sản phẩm và dịch vụ và gia tăng cơ hội để họ đổi mới và phát triển. Do đó, các nhà cung cấp dịch vụ doanh nghiệp làm việc chặt chẽ với các khách hàng doanh nghiệp sử dụng dịch vụ của họ nhưng thường không tương tác với các khách hàng cá nhân hoặc người dùng cuối được các khách hàng doanh nghiệp đó phục vụ.

LBVQLNTD 2022 áp đặt nhiều nghĩa vụ mới khác nhau đối với các doanh nghiệp, chẳng hạn như các yêu cầu phải có được sự đồng ý trước của người tiêu dùng để sử dụng dữ liệu cá nhân của họ và cập nhật hoặc xóa dữ liệu cá nhân của người tiêu dùng theo yêu cầu. Tuy nhiên, nhiều nhà cung cấp dịch vụ doanh nghiệp không có đủ năng lực để thực hiện các nghĩa vụ đó vì họ chỉ có quyền truy cập hạn chế vào dữ liệu khách hàng doanh nghiệp của mình, bao gồm cả danh tính người tiêu dùng cá nhân hoặc chi tiết liên hệ. Để lấy ví dụ, quyền truy cập của nhà cung cấp dịch vụ doanh nghiệp và kiến thức về dữ liệu đó thường bị hạn chế bởi các biện pháp kiểm soát quyền riêng tư và bảo mật được tích hợp trong các sản phẩm và dịch vụ của họ và được thực thi theo các điều khoản hợp đồng giữa nhà cung cấp và khách hàng doanh nghiệp của họ. Hơn nữa, chính khách hàng doanh nghiệp thường giữ mối quan hệ với người dùng cuối cá nhân (không phải nhà cung cấp dịch vụ doanh nghiệp). Việc buộc các nhà cung cấp dịch vụ doanh nghiệp phải tuân theo những nghĩa vụ này sẽ không chỉ là không khả thi về mặt kỹ thuật và thực tế mà còn có thể khiến họ vi phạm các nghĩa vụ theo hợp đồng và các nghĩa vụ pháp lý khác.

---

[3] Cách Phần mềm Doanh nghiệp Trao quyền cho các Doanh nghiệp trong nền Kinh tế theo hướng dữ liệu, tháng 1 năm 2021, https://www.bsa.org/files/policy-filings/011921bsaenterprisesoftware101.pdf và **được đính kèm với văn bản này.**

[4] Tiêu chuẩn Toàn cầu: Phân biệt giữa Bên Kiểm soát và Bên Xử lý trong Pháp luật về Quyền riêng tư tháng 3 năm 2020, https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf và **được đính kèm với văn bản này.**

[5] LBVQLNTD 2022, Điều 3.2. Tổ chức, cá nhân kinh doanh là tổ chức, cá nhân thực hiện một, một số hoặc tất cả các công đoạn của quá trình đầu tư, từ sản xuất đến tiêu thụ sản phẩm hoặc cung cấp dịch vụ trên thị trường nhằm mục đích sinh lợi, bao gồm: a) Thương nhân, thương nhân nước ngoài theo quy định của Luật Thương mại; b) Cá nhân hoạt động thương mại độc lập, thường xuyên, không phải đăng ký kinh doanh;

[6] LBVQLNTD 2022, Điều 3.11. Nền tảng trung gian trực tuyến là các hệ thống thông tin do tổ chức, cá nhân thiết lập và vận hành để cung cấp môi trường trên không gian mạng cho các tổ chức, cá nhân khác giao dịch với người tiêu dùng.

[7] LBVQLNTD 2022, Điều 3.12. Nền tảng trung gian trực tuyến lớn là nền tảng tác động đến số lượng đủ lớn người tiêu dùng sử dụng dịch vụ trực tuyến trên nền tảng theo quy định của Chính phủ.

Ví dụ, theo Điều 21 trong dự thảo, các nghĩa vụ cung cấp các giải pháp kỹ thuật được đặt ra để ngăn chặn các dịch vụ khỏi việc quấy rối người tiêu dùng. Trong trường hợp nhà cung cấp dịch vụ doanh nghiệp được khách hàng doanh nghiệp của họ sử dụng để tiếp cận người dùng cuối cá nhân của họ, nhà cung cấp dịch vụ doanh nghiệp đó không có tư cách can thiệp vào hành động của khách hàng doanh nghiệp liên quan đến người dùng cuối của khách hàng đó. Không nên áp đặt các nghĩa vụ đối với nhà cung cấp dịch vụ doanh nghiệp trong các tình huống như vậy.

Hơn nữa, việc áp đặt các nghĩa vụ đối mặt người tiêu dùng lên các nhà cung cấp dịch vụ doanh nghiệp không làm tăng thêm quyền riêng tư của người tiêu dùng. Ví dụ: nếu nhà cung cấp dịch vụ doanh nghiệp được yêu cầu phải có sự đồng ý của người dùng cuối cá nhân, thì trường hợp thường xảy ra là bên kiểm soát dữ liệu đã có được sự đồng ý để xử lý dữ liệu của họ. Việc yêu cầu nhà cung cấp dịch vụ doanh nghiệp đạt được sự đồng ý giống nhau cho cùng một quá trình xử lý giống nhau không chỉ mang tính trùng lặp mà còn có khả năng buộc nhà cung cấp dịch vụ doanh nghiệp liên hệ với những người dùng cuối cá nhân vốn không quen biết gì với nhà cung cấp dịch vụ doanh nghiệp. Điều này có thể gây nhầm lẫn cho người dùng cuối cá nhân và có thể làm suy yếu quyền riêng tư của người dùng cuối cá nhân vì bên kiểm soát dữ liệu có khả năng phải tiết lộ thông tin liên hệ của người dùng cuối cá nhân cho nhà cung cấp dịch vụ doanh nghiệp (hoặc ủy quyền cho nhà cung cấp truy cập dữ liệu mà bình thường họ không phải truy cập) để cho phép nhà cung cấp tiếp cận với người tiêu dùng.

Những lo ngại trên xuất phát từ các định nghĩa quá rộng về "tổ chức kinh doanh", "nền tảng trung gian trực tuyến" và "nền tảng trung gian trực tuyến lớn". Ví dụ, định nghĩa về "tổ chức kinh doanh" bao hàm *tất cả* các thực thể kinh doanh tham gia vào chuỗi cung ứng dẫn đến việc hàng hóa hoặc dịch vụ được đưa tới người tiêu dùng. Điều này sẽ bao gồm các nhà cung cấp dịch vụ đám mây (**CSPs**) cung cấp các nền tảng, cơ sở hạ tầng hoặc dịch vụ lưu trữ dựa trên đám mây cho các doanh nghiệp, nhưng họ không kiểm soát được cách thức khách hàng doanh nghiệp của họ giao dịch hoặc tương tác với người tiêu dùng. Tương tự, có thể nói CSPs cung cấp "môi trường trong không gian mạng" cho người bán giao dịch với người tiêu dùng theo định nghĩa của "nền tảng trung gian trực tuyến", nhưng không có quyền kiểm soát cách thức người bán tổ chức mối quan hệ của họ với người tiêu dùng.

Vì những lý do nêu trên, BSA khuyến nghị rằng LBVQLNTD 2022 chỉ nên áp dụng cho các công ty cung cấp dịch vụ đối mặt người tiêu dùng, làm việc trực tiếp với người dùng cuối cá nhân và thông tin cá nhân của họ, chứ không phải cho các nhà cung cấp dịch vụ doanh nghiệp. Điều này có thể đạt được bằng cách sửa đổi các định nghĩa quá rộng về "tổ chức kinh doanh", "nền tảng trung gian trực tuyến" và "nền tảng trung gian trực tuyến lớn" (ví dụ: bằng cách nêu rõ rằng các định nghĩa này không áp dụng cho một tổ chức cung cấp dịch vụ được thiết kế chủ yếu cho và được sử dụng bởi doanh nghiệp/khách hàng doanh nghiệp).

Phân biệt bên kiểm soát dữ liệu và bên xử lý dữ liệu, và miễn các nghĩa vụ cụ thể cho bên xử lý dữ liệu

LBVQLNTD 2022 hiện không phân biệt giữa bên kiểm soát dữ liệu và bên xử lý dữ liệu. BSA khuyến nghị nên quy định về sự khác biệt này, vì việc phân bổ trách nhiệm giải trình rõ ràng giữa bên kiểm soát dữ liệu và bên xử lý dữ liệu là cần thiết để thiết lập và thực thi các nghĩa vụ liên quan đến quyền riêng tư.

Bằng cách phân biệt giữa bên kiểm soát dữ liệu và bên xử lý dữ liệu, LBVQLNTD 2022 có thể điều chỉnh rõ ràng các nghĩa vụ cho các loại công ty khác nhau dựa trên vai trò của các công ty đó trong việc thu thập và sử dụng thông tin cá nhân của người dùng cuối cá nhân. Sự khác biệt này đặc biệt quan trọng trong nền kinh tế kỹ thuật số ngày nay, nơi một cá nhân có thể sử dụng dịch vụ từ một công ty đối mặt người tiêu dùng, nhưng công ty đó có khả năng phụ thuộc vào nhiều nhà cung cấp dịch vụ doanh nghiệp để lưu trữ, phân tích và xử lý dữ liệu liên quan đến dịch vụ đó.

Chúng tôi có những lo ngại lớn rằng LBVQLNTD 2022 có thể làm suy yếu quyền riêng tư của người tiêu dùng nếu áp đặt các nghĩa vụ liên quan đến việc làm việc trực tiếp với người tiêu dùng lên các bên xử lý dữ liệu vốn không có mối quan hệ trực tiếp với người dùng cuối cá nhân. Những lo ngại

này đặc biệt liên quan đến các nghĩa vụ liên quan tới **sự đồng ý, thông báo và phản hồi các yêu cầu về quyền của người tiêu dùng.**[8]

- *Sự Đồng ý và Thông báo*. Các nghĩa vụ về sự đồng ý và thông báo là những nghĩa vụ đối mặt người tiêu dùng chính mà được đặt một cách thích hợp lên bên kiểm soát dữ liệu, không phải bên xử lý dữ liệu. Người dùng cuối cá nhân của các dịch vụ thường tương tác với những bên kiểm soát mà cung cấp dịch vụ — và đúng ra có thể mong đợi bên kiểm soát yêu cầu sự đồng ý của họ để xử lý thông tin cá nhân của họ cho các mục đích nhất định và cung cấp thông báo thích hợp về cách những bên kiểm soát sẽ xử lý thông tin cá nhân của họ. Tuy nhiên, việc yêu cầu bên xử lý dữ liệu cũng phải có được sự đồng ý và thông báo cho người dùng cuối cá nhân vì những mục đích đó không chỉ dẫn đến những thông báo và yêu cầu đồng ý trùng lặp từ nhiều công ty cho cùng một hoạt động xử lý mà còn có nguy cơ gây nhầm lẫn cho người dùng cuối cá nhân và dẫn đến hiện tượng "nhấp chuột mệt mỏi" — trường hợp mà người dùng cuối ngập tràn trong các thông báo và yêu cầu lặp đi lặp lại, làm giảm thiểu tính hiệu quả của các thông báo và yêu cầu trong việc thông báo cho người dùng cuối cá nhân về các vấn đề liên quan và trong việc xác nhận mong muốn và kỳ vọng của họ.
- *Trả lời các Yêu cầu về Quyền lợi Người tiêu dùng*. Các công ty làm việc trực tiếp với người tiêu dùng cũng ở vị trí thích hợp nhất để phản hồi các yêu cầu về quyền lợi người tiêu dùng, đồng thời không tạo ra các mối lo ngại về quyền riêng tư và bảo mật có thể phát sinh khi các nghĩa vụ này được đặt lên bên xử lý dữ liệu. Điều này là do việc phản hồi các yêu cầu về quyền lợi người tiêu dùng đối với việc ngừng sử dụng hoặc tiết lộ thông tin cá nhân thường đòi hỏi việc xác thực danh tính của người dùng cuối là cá nhân đưa ra yêu cầu và sự hiểu biết về việc liệu thông tin được yêu cầu có nên được cung cấp hay không. Bên kiểm soát dữ liệu cá nhân nên đưa ra những quyết định nói trên vì bên kiểm soát dữ liệu tương tác trực tiếp người dùng cuối là cá nhân, quyết định thời điểm và lý do thu thập thông tin cá nhân cũng như phản hồi các yêu cầu về quyền của người tiêu dùng nên bên kiểm soát dữ liệu. Hơn nữa, bên kiểm soát dữ liệu ở vị trí thích hợp hơn để quyết định xem có lý do gì để từ chối yêu cầu của người dùng cuối cá nhân hay không. Các nghĩa vụ này không phù hợp với các bên xử lý dữ liệu vì họ thường không được biết bản chất của dữ liệu mà họ đang xử lý hoặc mục đích thực hiện việc xử lý đó. Ngoài ra, như đã nêu trước đó, theo hợp đồng bên xử lý dữ liệu có thể bị cấm truy cập vào dữ liệu mà họ lưu trữ hoặc xử lý cho bên kiểm soát dữ liệu và họ có thể thiết kế các hoạt động xử lý của họ để giảm thiểu lượng thông tin cá nhân mà họ cần truy cập — tất cả điều này đều bảo vệ sự riêng tư của dữ liệu đó tốt hơn. Do đó, việc yêu cầu bên xử lý dữ liệu phản hồi các yêu cầu của người dùng cuối cá nhân sẽ tạo ra rủi ro về bảo mật dữ liệu và quyền riêng tư của người tiêu dùng vì điều này đòi hỏi bên xử lý phải truy cập thông tin cá nhân, bao gồm dữ liệu cần thiết để nhận dạng cá nhân, mà đáng lẽ họ không cần phải truy cập.

Do đó, BSA khuyến nghị <u>miễn</u> các nghĩa vụ sau cho các bên xử lý dữ liệu:

- **Cung cấp thông báo cho người tiêu dùng cá nhân của khách hàng của bên xử lý dữ liệu (khách hàng là doanh nghiệp đối mặt người tiêu dùng) và nhận được sự đồng ý của người tiêu dùng cá nhân để thu thập hoặc sử dụng thông tin cá nhân của họ;**[9]
- **Thông báo cho người tiêu dùng cá nhân của khách hàng của bên xử lý dữ liệu (khách hàng là doanh nghiệp đối mặt người tiêu dùng) khi có thay đổi về mục đích và phạm vi được quy định trong thông báo/yêu cầu sự đồng ý ban đầu;**[10] **và**

[8] LBVQLNTD 2022, Điều 9 (Thông báo khi thu thập thông tin cá nhân của người tiêu dùng), Điều 10 (Sử dụng thông tin cá nhân của người tiêu dùng), and Điều 12 (Kiểm tra, cập nhật, điều chỉnh, chuyển giao hoặc hủy bỏ thông tin cá nhân của người tiêu dùng).

[9] LBVQLNTD 2022, Điều 9 và 10.

[10] LBVQLNTD 2022. Điều 10.

- **Đáp ứng các yêu cầu từ người tiêu dùng cá nhân của khách hàng của bên xử lý dữ liệu (khách hàng là doanh nghiệp đối mặt người tiêu dùng) để kiểm tra, cập nhật, sửa chữa, chuyển giao hoặc huỷ bỏ thông tin cá nhân của họ.[11]**

Nói một cách rõ ràng hơn, các nghĩa vụ trên **chỉ nên** áp dụng đối với khách hàng doanh nghiệp giao dịch trực tiếp với người tiêu dùng (bên kiểm soát) chứ không phải nhà cung cấp dịch vụ doanh nghiệp (bên xử lý).

Loại bỏ Điều 9 về yêu cầu sự đồng ý

Theo Điều 9, LBVQLNTD 2022 công nhận "sự đồng ý" là cơ sở duy nhất để thu thập và xử lý thông tin cá nhân của người tiêu dùng. Tuy nhiên, dự thảo mới nhất của Nghị định BVDLCN đã đề xuất một số trường hợp ngoại lệ đối với việc xử lý mà không có sự đồng ý.[12] Do đó, nếu quy định rằng "sự đồng ý" là cơ sở duy nhất để xử lý thông tin cá nhân, LBVQLNTD 2022 đang mâu thuẫn với dự thảo Nghị định BVDLCN. Xung đột pháp luật sẽ khiến các doanh nghiệp bối rối trong việc xác định phương hướng tuân thủ hoạt động bảo vệ dữ liệu cá nhân tại Việt Nam và có thể dẫn đến việc vô tình không tuân thủ các nghĩa vụ bảo vệ dữ liệu của họ. Hơn nữa, do LBVQLNTD 2022 và Nghị định BVDLCN được giám sát và quản lý bởi các Bộ khác nhau, khung pháp lý đối với hoạt động bảo vệ thông tin cá nhân ở Việt Nam có thể trở nên rời rạc do việc thực thi thiếu nhất quán, dẫn đến sự nhầm lẫn về quy định pháp luật.

Có thể tránh được sự nhầm lẫn về quy định này nếu các điều khoản tạo tiền đề cho hoạt động xử lý thông tin cá nhân *chỉ* được quy định trong luật bảo vệ dữ liệu cá nhân, cụ thể như Nghị định BVDLCN, thay vì được quy định trong *cả* Nghị định BVDLCN và luật khác như LBVQLNTD 2022. Do đó, BSA khuyến nghị loại bỏ Điều 9 ra khỏi LBVQLNTD 2022 để tránh nhầm lẫn và xung đột với dự thảo Nghị định BVDLCN.

Kết luận

Chúng tôi xin cảm ơn Bộ CT vì đã cho chúng tôi cơ hội được đóng góp ý kiến đối với LBVQLNTD 2022 và sự quan tâm xem xét của Bộ CT đối với các ý kiến nêu trên của chúng tôi. Chúng tôi hy vọng rằng những mối quan tâm và khuyến nghị của chúng tôi sẽ hỗ trợ việc phát triển khuôn khổ mục tiêu để bảo vệ người tiêu dùng. Xin vui lòng liên hệ với tôi nếu Quý Bộ có bất kỳ câu hỏi nào liên quan đến thư góp ý này hoặc cần thêm sự hỗ trợ.

Trân trọng,

Tham Shen Hong

Tham Shen Hong

Giám đốc, Chính sách – Khu vực Châu Á – Thái Bình Dương

[11] LBVQLNTD 2022, Điều 12.

[12] Nghị định BVDLCN, Điều 10.

The Software Alliance

BSA

How Enterprise Software Empowers Businesses in a Data-Driven Economy

B2B software enables business customers to do what they do best—faster, smarter, and more efficiently.

Enterprise Software Supports Businesses' Operations

Enterprise software—or business-to-business (B2B) software—**enables** the operations of other companies. It helps organizations of all sizes and across all industries operate more safely and efficiently, enhance product and service development, and increase opportunities to innovate and grow.

The enterprise software industry supports a wide range of organizations across the world, including SMEs and large companies; local and central governments; hospitals, schools, and universities; and non-profits. By **offering trusted and responsible software solutions** to support their business clients' data-processing needs, enterprise software companies enable other organizations to service their own customers in turn.



Enterprise software optimizes the use of digital technology to support and improve business operations, empowering other companies to focus on what they do best, such as R&D and product design.



In Europe, almost **80 percent of large companies** and **35 percent of SMEs** use information-sharing software.[1]

Enterprise Software Helps Businesses Benefit From Digital Transformation

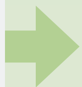
Organizations in every sector of the economy increasingly rely on cutting-edge software to **run, facilitate, improve, and optimize their operations** every single day. Governments, public administrations, schools, and hospitals are also increasingly adopting these tools. Enterprise software underpins human resources and payroll operations; billing and financial transactions; research and development; product design; workforce collaboration, communication, and messaging; customer relations; and logistics and supply-chain management, among many other business services.



38 percent of small businesses in the **United States** cited increased sales and revenue as a benefit associated with using digital tools.[2]



Australian businesses are using more cloud than ever—**42 percent of businesses** across 2017–2018, up from 31 percent in 2015–2016.[3]



In times of crisis, such as the global outbreak of COVID-19, enterprise software tools help coordinate public health safety responses, maintain essential services, and support economic continuity.

ENTERPRISE (B2B) SOFTWARE PROVIDES CLIENT SOLUTIONS THAT:



Operate and Optimize Business Services (including responsibly handling and moving information globally)



Protect and Secure Data and Business Information (including providing strong, accountable privacy and security safeguards)



Innovate and Expand Beyond Existing Capabilities (by using cognitive solutions such as analytics and artificial intelligence to better address customers' needs)

[1] EU DESI Index 2020, https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi.

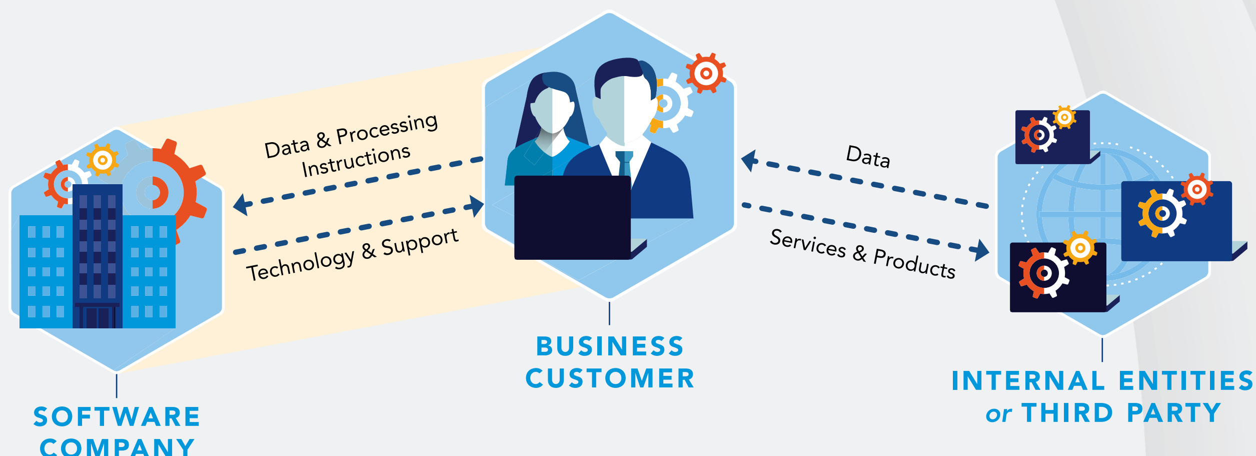
[2] https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/connected-small-businesses.html.

[3] Characteristics of Australian Business, https://www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2017-18.

Enterprise Software Is Built on Transparency and Trust

Enterprise software companies and their business customers negotiate their relationship in contracts and licensing agreements to ensure they best address their clients' individual needs. **Enterprise software companies monetize their technologies and not the data of their customers.**

Enterprise software services, such as cloud computing, are used primarily for business-to-business purposes and are not consumer facing. **The business customers control their data and direct how it will be used.** Enterprise software companies do not have unfettered access to the data stored in their cloud infrastructure or service. Access and use of such data is reserved for the benefit and sole purpose of their customers.



Enterprise software companies operate under strong existing legislative requirements of data handling. Across the world, legal obligations often include accountability measures and technical safeguards that ensure enterprise software companies provide robust assurances of trust for their customers. Enterprise software companies also develop innovative, tailored, or customizable solutions for clients that are highly regulated, for example, in the health, financial, automotive, aeronautic, and telecom sectors and the semiconductor industry.[4]

For instance, machine learning solutions can use data gathered across countries to create fraud detection systems in the financial sector.

Enterprise software helps reduce legal and operational risks for business customers who can be confident they are using tried and tested software products, with appropriate remedies and support, without having to develop their own software in-house. Enterprise software companies also often provide tools to facilitate their customers' compliance, for instance on privacy, consumer protection, cybersecurity, anti-money laundering, or energy efficiency.

4 See Cross-Border Data Flows: Enabling Local Economies and Driving E-Commerce, https://www.globaldataalliance.org/downloads/WTOEventSummary20200702.pdf.

How to Create a Successful, Responsible, Software-Enabled Economy



STRONG PRIVACY PROTECTIONS

Privacy is essential to building trust. Software-enabled business operations increasingly rely on data—and, in some cases, personal data—to function. As a result, data protection frameworks that create a user-centric approach to privacy must ensure the use of personal data is clear, transparent, and consistent with customers' expectations. Privacy laws should create robust obligations for all companies and organizations that handle individuals' personal data. This would ensure companies act responsibly while being able to pursue legitimate business interests.



CYBERSECURITY

Software innovation continues to connect people across the world. These online connections create efficiencies and spur economic growth, but they also create vulnerabilities that bad actors can exploit if the proper security measures are not in place. Addressing cybersecurity challenges requires innovative tools and practices to defend the integrity, confidentiality, and resilience of the connected ecosystem. One important tool is the ability to use the strongest available encryption technology when appropriate.



CROSS-BORDER DATA FLOWS

Cross-border data flows are necessary for companies to operate globally; leverage their resources and footprint across locations; innovate; and provide services to their customers, across sectors and geographies. For enterprise software companies and their business customers, the ability to transfer, and process, data globally is pivotal in ensuring the quality, reliability, security, personalization, and efficiency of service.



RISK-BASED AND TECHNOLOGY-NEUTRAL APPROACH

Software technologies evolve every day, pushing the boundaries of the benefits that technology can bring to organizations and people. Given the fast-paced nature of this industry and its adoption by customers, laws and regulations should strive to provide legal certainty, be outcome-based, and adopt a risk-based and technology-neutral approach, building on legal frameworks that already apply. Any new policy should set clear compliance goals and enable companies to adapt their practices and safeguards to the best-suited approach given their business model, the nature of their activity, their position in the value chain when contracted by others, and their risk profile vis-à-vis the established objective.



INTERNATIONAL CONVERGENCE

The value of the data-driven economy is in the ability of companies to operate across borders, reach new markets, and service customers regardless of location. Building on each region's own legal and cultural legacy, convergence of rules on privacy, cybersecurity, or data governance and compatibility of mechanisms play a critical role in growing cross-border business that increasingly rely on enterprise software around the world.

The Software Alliance

BSA



The Global Standard: Distinguishing Between Controllers and Processors in Privacy Legislation

Comprehensive privacy legislation must create strong obligations for all companies that handle consumer data. These obligations will only be strong enough to protect consumer privacy and instill trust, though, if they reflect how a company interacts with consumer data.

Privacy laws worldwide distinguish between two types of companies: (1) businesses that decide *how* and *why* to collect consumer data, which act as **controllers** of that data and (2) businesses that process the data on *behalf of* another company, which act as **processors** of that data

This fundamental distinction is critical to a host of global privacy laws, including the European Union's General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). Both types of businesses have important responsibilities and obligations, which should be set out in any legislation.

Who Handles Consumer Data?



Personal Data

Products & Services



Data & Processing Instructions

Processed Data



CONSUMER

Individuals whose personal data is collected and used by a controller

EXAMPLES

Consumers who shop at retail stores, buy products online, or share information on social media platforms.

CONSUMERS SHOULD HAVE THE RIGHT TO:

- **Know** what type of data a controller collects — and why
- **Say no,** and opt out of broad types of use, not just sale
- **Access** information about them
- **Correct** that information
- **Delete** that information
- Have their data **securely protected**
- Have their data used **consistent with their expectations**

CONTROLLER

Decides whether and how to collect data from consumers, and the purposes for which that data is used

EXAMPLES

Companies that interact directly with consumers, such as hotels, banks, retail stores, travel agencies, and consumer-facing technology providers.

CONTROLLERS ARE RESPONSIBLE FOR:

Obtaining any consent needed to process a consumer's data

Responding to consumer requests for access, correction, or deletion

Using data consistent with the consumers' expectation

PROCESSOR

Processes data on behalf of a controller, pursuant to the controller's instructions

EXAMPLES

Companies that provide business-to-business products like cloud computing, and vendors like printers, couriers, and others that process data at the direction of another company.

PROCESSORS ARE RESPONSIBLE FOR:

Processing data consistent with a controller's instructions

Adopting appropriate safeguards designed to protect data security

Controllers and processors should have role-dependent responsibilities to ensure consumers' privacy and security are protected.

Privacy Laws Worldwide Distinguish Between Controllers and Processors

Privacy laws worldwide reflect the basic distinction between companies that decide to collect and use data about individuals and companies that only process such data.

Companies that decide how and why to collect consumer data.	Companies that process consumer data at the direction of others.
GDPR: Controllers Determine the "purposes and means" of processing.	**GDPR: Processors** Handle personal data "on behalf of" a controller.
CCPA: Businesses Determine the "purposes and means" of processing.	**CCPA: Service Providers** Handle personal information "on behalf of" businesses.

This distinction is crucial to a host of privacy laws beyond the GDPR and CCPA. In addition, leading international privacy standards, including ISO 27701, and voluntary frameworks that ensure data can be transferred across national borders, such as the APEC Cross Border Privacy Rules, also distinguish between controllers and processors.

EXAMPLE

A business contracts with a printing company to create invitations to an event. The business gives the printing company the names and addresses of the invitees from its contact database, which the printer uses to address the invitations and envelopes. The business then sends out the invitations.

The business is the controller of the personal data processed in connection with the invitations. The business decides the purposes for which the personal data is processed (to send individually-addressed invitations) and the means of the processing (mail merging the personal data using the invitees' addresses). The printing company is the processor handling the personal data pursuant to the business's instructions. The printing company cannot sell the data or use it for other purposes, such as marketing. If the printing company disregarded those limits and used the data for its own purposes, it would become a controller and be subject to all obligations imposed on a controller.

Why Is the Distinction Between Controllers and Processors Important to Protecting Consumer Privacy?

Distinguishing between controllers and processors ensures that privacy laws impose obligations that reflect a company's role in handling consumer data. This helps safeguard consumer privacy without inadvertently creating new privacy or security risks.

Data Security. Controllers and processors should both have strong obligations to safeguard consumer data.

» Placing this obligation on both types of companies ensures consumer data is protected.

» Controllers and processors should both employ reasonable and appropriate security measures, relative to the volume and sensitivity of the data, size, and nature of the business, and the cost of available tools.

Consumer Rights Requests. Responding to important consumer rights requests—such as requests to access, correct, or delete personal data—requires knowing what is in that data.

» Controllers interact with consumers and decide when and why to collect their data. For that reason, laws like the GDPR and CCPA require controllers to respond to consumer rights requests. Moreover, controllers must decide if there is a reason to deny a consumer's request, such as when a consumer asks to delete information subject to a legal hold.

» Processors, in contrast, often do not know the content of the data they process, and may be contractually prohibited from looking at it. It is not appropriate for processors to respond directly to a consumer's request—which creates both security risks (by providing data to consumers they do not know) and privacy risks (by looking at data they otherwise would not). Processors should instead provide controllers with tools the controller can use to collect data needed to respond to a consumer's request.